

MEMORANDUM

Date : December 4, 2008

To : Matthew Paulin, Deputy Director, Administrative Services Division (ASD)
Steve Westerman, Deputy Director, Information Systems Division (ISD)

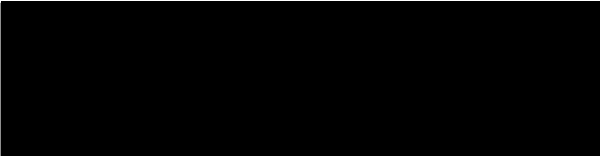
From : Executive Division -Audits Office

Subject: **National Automated Clearing House Association (NACHA) Audit - Report**

The Audits Office presents its final audit report of the NACHA Audit for the year ending December 2008. The audit report entitled "*Final Audit Report - National Automated Clearing House Association Audit*" is attached for your information. Please note the attached report includes excerpts of ASD's and ISD's response to our findings, as well as our response evaluation. We have included the responses received from ASD and ISD in its entirety as Exhibits 1 & 2 at the end of the report.

At six months we request that ASD and ISD provide us with a written status on the corrective actions planned and implemented for the findings.

We thank ASD and ISD and their staff during this review for their cooperation and courtesy extended to our auditors. If you have any questions please contact me at (916) 657-5828.



GRACE M. RULE-ALI, Manager
Information Systems-Requester Audit Section
(916) 657- 5828



Attachment

cc: Michael Ferrara, AAP, Vice President, Union Bank of California
George Valverde, Director, DMV
Ken Miyao, Chief Deputy Director, DMV
S. Paulette Johnson, Chief Information Privacy & Security Officer, DMV
Jeff Mansur, Chief, Financial Services Branch, DMV

Union Bank of California

Annual WEB Audit Certification 2008

I certify that our business has completed the ACH WEB Originator Annual Audit in compliance with the *ACH Operating Rules*, Appendix Eight.

DATE December 4, 2008		
CUSTOMER NAME Department of Motor Vehicles		CUSTOMER TAX ID NUMBER 
ADDRESS 2415 1 st Avenue	CITY Sacramento	STATE CA
CUSTOMER CONTACT (name and title) Jerry McClain, Chief Audits Office	TELEPHONE (916) 657-0455	
SIGNATURE 	E-MAIL ADDRESS jmcclain@dmv.ca.gov	

FINAL AUDIT REPORT
CALIFORNIA DEPARTMENT OF MOTOR VEHICLES
NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION

TABLE OF CONTENTS

COVER MEMO.....	i
EXECUTIVE SUMMARY.....	1
BACKGROUND.....	2
OBJECTIVES, SCOPE AND METHODOLOGY.....	2
FINDINGS AND RECOMMENDATIONS.....	3-5
 FINDING #1 UNSECURED PHYSICAL LOCATION OF PERSONAL COMPUTERS USED TO PROCESS ELECTRONIC FUNDS TRANSFER (EFT) TRANSACTIONS	
 FINDING #2 CUSTOMER FINANCIAL INFORMATION CAN BE TRANSMITTED WITH AN ENCRYPTION LEVEL LESS THAN RECOMMENDED STANDARD	
 FINDING #3 NO EFT DATA RETENTION POLICY AND MONITORING SCHEDULES	
CONCLUSION	6
EXHIBIT 1 ASD RESPONSE.....	7
EXHIBIT 2 ISD RESPONSE.....	8

EXECUTIVE SUMMARY

The California Department of Motor Vehicles (DMV) provides services to customers via the Internet, mail, and telephone or by visiting a DMV Field Office. This audit is focusing solely on electronic payments provided via the Internet using the National Automated Clearing House Association (NACHA) electronic funds transfer (EFT) payment applications. Adding this alternative payment option allows customers without a credit card, but who have a bank account, to process transactions from the convenience of home. In June 2006 and June 2007, DMV implemented the on-line EFT payment option for customers. The current EFT renewal transactions via the Internet include:

- Renewal of a driver license (Drivers License Renewal By Internet [DL-RBI])
- Renewal of a vehicle registration (Vehicle Registration Renewal By Internet [VRIR])

DMV processes the on-line EFT payments using the Automated Clearing House (ACH) network. NACHA requires entities that provide ACH services to conduct an annual audit of compliance in accordance with the requirements of Appendix Eight of the 2008 ACH Rules Book no later than December 1st of each year.

We conducted audit fieldwork at DMV and the Department of Technology Services (DTS) during September and October 2008. Our audit included an examination of MV's on-line EFT payment processes. The scope of the review included physical security, fraud detection systems, verification of routing numbers, protection of customer's information, personnel and access controls, and existing network security to protect the financial information DMV receives from its customers.

Our evaluation found that current security controls in effect at DMV as of October 23, 2008, are sufficient to meet the security objectives of this audit, except as noted in the *Findings and Recommendations* section of this report however, they are summarized below:

- Unsecured physical location of personal computers used to process Electronic Funds Transfer (EFT) Transactions.
- Customer financial information can be transmitted with an encryption level less than recommended standard.
- No EFT data retention policy and monitoring schedules.

BACKGROUND

NACHA is a non-profit association that represents more the 11,000 financial institutions and develops operating rules and business practices for the ACH Network. ACH

processes include electronic payments in the areas of Internet commerce, electronic bill and invoice payment, e-checks, and financial electronic data interchange. ACH Operating Rules require an "Originator" of "WEB Internet-Initiated Entry" meets the requirements imposed by the various ACH rules and regulations, as well as State and Federal statutes.

In June 2006, the DMV implemented e-check as a payment option for customers who renew their Driver License and Vehicle Registration via the Internet. In December 2007, NACHA notified DMV that ACH rules require an originator of a "WEB Internet-Initiated Entry" conduct an annual audit. However, due to late notification, the ACH Network granted DMV an extension to December 1, 2008. Therefore, this audit will cover the time period July 1, 2007 through June 30, 2008.

OBJECTIVES, SCOPE AND METHODOLOGY

The audit objectives were to determine if DMV's Web-based services comply with the requirements set forth in the 2008 ACH Rules book as well as applicable statutes and regulations stated in the Government code. Accordingly, we developed an audit plan to determine whether:

- The Department adheres to the provisions of the NACHA 2008 ACH Rules Book and complies with applicable rules and regulations.
- Fraud Detections Systems are adequate to safeguard customer information.
- Proper procedures are in place to verify the validity of routing numbers.
- Verification of receivers' identity to protect against unauthorized access takes place.
- Adequate physical security exists to protect against theft, tampering or damage.
- Personnel and access controls to protect against unauthorized access and use are present.
- Network security to ensure secure capture, storage and distribution is in use.

The scope of the review included auditing to ensure authentication, proper access and use, and adequate security controls in place to protect the financial information DMV receives from its customers.

We conducted this audit in accordance with *Government Auditing Standards* promulgated by the United States General Accountability Office. Our evaluation and methodology included such demonstrations and observations as considered necessary to meet our objectives. Our procedures included interviews with applicable DMV and DTS staff and management; physical observation of DMV's Electronic Payment Services (E-Pay Services) Unit; demonstration of the Driver License and Vehicle Registration applications used to process on-line EFT payment transactions and, review and verification of documentation.

FINDING #2 – CUSTOMER FINANCIAL INFORMATION CAN BE TRANSMITTED WITH AN ENCRYPTION LEVEL LESS THAN RECOMMENDED STANDARD

Condition: The department's EFT Internet renewal applications support and do not prohibit customers from transmitting their banking information at an encryption standard less than the recommended standard.

Currently, the Department is set up for 256-bit, AES (Advanced Encryption Standard) encryption, and TLS1 (Transport Layer Security). However, the DMV Internet renewal applications also allow a lower 40-bit encryption standard as demonstrated by a DMV Information Systems Division programmer. The NACHA *Operating Rules* require, at a minimum, customers EFT payment transmissions be submitted at an encryption level equivalent to 128-bit encryption. Although the DMV EFT Internet renewal applications *recommend* using 128-bit encryption, the applications do not prohibit DMV customers from submitting their sensitive banking information using the less secure 40-bit encryption standard.

Allowing DMV customers to submit their banking information at the less secure 40-bit encryption level could expose the customers banking information to security risks and compromise.

Criteria: The 2008 ACH Rules Corporate Edition, Section IV – Special Topics, Chapter XVI – Internet-Initiated Entries, Sub-Section E – ACH Data Security Requirements states in part, “For all ACH transactions that involve the exchange or transmission of banking information (which includes, but is not limited to, an entry, entry data, a routing number, an account number, and a PIN or other identification symbol) via an Unsecured Electronic Network, the NACHA *Operating Rules* require that such banking information be either (1) encrypted using a commercially reasonable security technology that, at a minimum, is equivalent to 128-bit RC4 encryption technology, or (2) transmitted via a secure session that utilizes a commercially reasonable security technology that provides a level of security that, at a minimum, is equivalent to 128-bit RC4 encryption technology.” “These encryption requirements must be employed prior to the key-entry and through the transmission of any banking information exchanged over such an Unsecured Electronic Network between (1) an Originator and a Receiver....”

Recommendation: We recommend that the program consider a modification to increase security of the EFT payment applications to safeguard DMV's customer's sensitive banking information from transmission at the less secure 40-bit encryption standard.

ISD Response: “Proposed Short-Term Solution”

- DLIR/VRIR Landing Page(s) enforcing 128-bit minimum encryption level
- Verbiage within the application warning customer of security risks
- Additional verbiage within the 'Terms' statement that customer must accept before continuing.....”

Our audit evaluation found, that taken as a whole, the current security controls in effect for DMV's Web based services meet the requirements set forth in the 2008 ACH Rules and applicable statutes. However, we identified reportable weaknesses as noted in the *Findings and Recommendations* section of this report. However, because of inherent limitations in control systems, errors or irregularities may occur and not be detected. Therefore, projection of any evaluation of systems to future periods are subject to risk because procedures may become inadequate due to changes in conditions, or the degree of compliance with the procedures may deteriorate.

FINDINGS AND RECOMMENDATIONS

FINDING #1 - UNSECURED PHYSICAL LOCATION OF PERSONAL COMPUTERS USED TO PROCESS ELECTRONIC FUNDS TRANSFER (EFT) TRANSACTIONS

Condition: The E-Pay Services Unit maintains four personal computers (PCs) used to process the on-line EFT payment transactions. We observed one PC in a secured room while the remaining three PCs are unsecured and located throughout the unit. We confirmed that the Information Privacy and Security Office (IPSO) did not approve an exemption for the three PCs in the unsecured location. The PCs unsecured physical location increases security risk for theft, tampering or damage. Moreover, DMV customer's financial information is subject to unauthorized use, malicious destruction, unintentional destruction of hardware or data is at risk.

Criteria: The 2008 ACH Rules Corporate Edition, section 8.3 K 14 states, in part "physical security exists to protect against theft, tampering or damage". There should be adequate security controls in place to protect customers' financial information.

Recommendation: To protect against theft, tampering or damage, relocate the three PCs to a secure location where access will be restricted. Access should be limited to employees who have a necessary business function. We recommend working with IPSO to ensure new location meets adequate physical security.

ASD Response: "....None of the EFT information is stored on the hard drives of these personal computers.....The Financial Services Branch will work with the Information Systems Division to add another level of password protection before the EFT information can be accessed through the personal computers; and to ensure that the servers accessed from the personal computers are physically located in a secured area."

Audit Office Response: We concur with ASD's corrective action plan. To evidence compliance in this area, we ask that ASD submit a written notification documenting the changes are implemented at a six month follow up.

“Proposed Long Term Solution

The Web Site Infrastructure (WSI) Portal project is targeted with a tentative implementation date of December 2009.....we have requested that DMV’s technical liaison group (SST) contact DTS to work on a solution whereby the application server would not allow a customer with a browser encryption level below the 128-bit minimum to continue processing an e-commerce transaction. Due to the restrictions on this type of enforcement, (e.g. There would not be a user friendly error page displayed, the customer would just receive a generic application server error), we would also have verbiage placed on several pages of the application (s) to warn customers about the minimum encryption level requirements and provide links to download the appropriate browsers. The WSI project team will be notified with the results of the TSST/DTS communication to ensure they implement a similar solution to this issue.

Audit Office Response: We concur with ISD’s corrective action plan. To evidence compliance in this area, we ask that ISD submit a written response documenting the changes implemented at a six month follow up.

FINDING #3 – NO EFT DATA RETENTION POLICY AND MONITORING SCHEDULES

Condition: ASD does not have a policy for data retention and monitoring schedules of its customers EFT data. The purpose of establishing an EFT data retention policy and monitoring schedules is to ensure that customer’s sensitive financial information is not stored longer than necessary, which could subject the information to security risks and compromise.

- An EFT data retention policy would provide management and staff guidance for information security to conform to business requirements, laws, and administrative policies. Further, the associated monitoring is verification that the established policy is working as intended.

Criteria: The 2008 ACH Rules Corporate Edition, Section IV – Special Topics, Chapter XVI – Internet-Initiated Entries, Sub-Section 4 – Risk Management Annual Security

“Audits (3) Network security to ensure secure capture, storage, and distribution states in part that:

- “A data retention schedule should be developed that covers the policies on how to handle the data from the time of capture to destruction.”
- “Retention schedules should be monitored to ensure that they are being met.”
- Receiver information should only be stored permanently if it is required by law, regulation, rule, or a governing organization.”
- “Data should not be stored longer than necessary.”

Recommendation: We recommend ASD develop a policy that defines retention and monitoring schedules for DMV customers EFT data from the time of capture to destruction. The policy should ensure that the customer’s financial information is not


stored longer than necessary and only stored permanently if it is required by law, regulation, rule, or a governing organization.

ASD Response: “.....By December 4, 2008, the Administrative Services Division will issue a draft of an EFT Data Retention Policy and Monitoring Schedule.....”

Audit Office Response: We concur with ASD’s corrective action plan. To evidence compliance in this area, we ask that ASD submit a copy of their EFT Data Retention Policy and Monitoring Schedule a six-month follow up.

CONCLUSION

The on-line EFT renewal payment options DMV offers its customers are designed to protect the customers’ financial information while still allowing the customer to process their on-line transactions electronically. The on-line EFT applications are designed with security features to authenticate authorized users, and associated payment transactions have adequate security controls in place to protect customers’ financial information. As such, the controls in place to protect DMV’s customer’s financial information are sufficient and functioning properly to fulfill the audit objectives. However, some ACH Rules have not been adequately enforced and monitored. Implementation of this report’s recommendations will improve security controls for the Department’s Web-based services.



GRACE M. RULE-ALI, Manager
Information Systems-Requester Audit Section
Audits Office
(916) 657-5828

October 23, 2008

Review Team:
Laura Lundgren, Supervisor
Carolyn Manuel, Auditor-in-Charge
Mark Prichard, Auditor

EXHIBIT 1
ASD Response

Memorandum

Date : November 24, 2008

To : Grace M. Rule-Ali, Manager
Audits Office
Information Systems-Requester Audit Section

From : Administrative Services Division

Subject : National Automated Clearing House Association Audit

On November 18, 2008, the Audits Office issued its draft report entitled "Draft Audit Report - National Automated Clearing House Association Audit." The audit report identified three findings. The Administrative Services Division is responding to findings #1 and #3. The Information Systems Division will address Finding #2 Customer Financial Information Can Be Transmitted with an Encryption Level Less than Recommended Standard.

Finding #1 – Unsecured Physical Location of Personal Computers Used to Process Electronic Funds Transfer (EFT) Transactions

Response - The Financial Services Branch accesses customer EFT payment information on servers outside of the accounting office area through the personal computers. None of the EFT information is stored on the hard drives of these personal computers. Therefore, there is no potential loss of EFT data through theft, tampering or damage of the personal computers. The Financial Services Branch will work with the Information Systems Division to add another level of password protection before the EFT information can be accessed through the personal computers; and to ensure that the servers accessed from the personal computers are physically located in a secured area.

Finding #3 – No EFT Data Retention Policy and Monitoring Schedules.

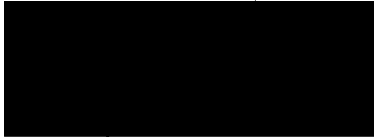
Response – Currently the Department maintains all EFT detail tables. By December 4, 2008, the Administrative Services Division will issue a draft of an EFT Data Retention Policy and Monitoring Schedule with the following guidelines.

- The department will delete customer EFT account and routing numbers from all files and databases maintained by the department within 60 days of the deposit of the payment in the department's bank account with certain exceptions.
- The department will maintain customer EFT account and routing numbers when the customer's account has insufficient funds or an invalid account that prevents the department from receiving payment. The department will retain this information for up to four years to ensure compliance with the collection

process in the State Administrative Manual and the Revenue and Taxation Code applicable to the collection of fees related to vehicle registration. After collection of the debt or the debt has proven to be uncollectible and written off, the department will delete the EFT account and routing information.

- The department will maintain information other than the EFT account and routing number sufficient to maintain a financial audit trail and customer record. The department will maintain financial information for the current fiscal year and four prior fiscal years.
- The policy related to EFT payment information from customers requires that management conduct periodic reviews of data retention to ensure the department is following the policy.

If you need additional information or have questions, please contact Jeff Mansur at 657-8141.



MATT PAULIN
Deputy Director

cc: S. Paulette Johnson
Jeff Mansur
Carolyn Manuel
Sandy Barriga

EXHIBIT 2
ISD Response

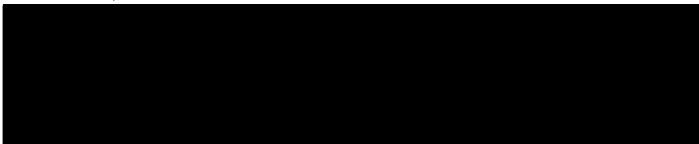
Memorandum

Date : December 4, 2008
To : Grace M. Rule-Ali
From : STEVEN J. WESTERMAN, Deputy Director
Information Systems Division
Subject : National Automated Clearing House Association (NACHA) Draft Audit Report

Please find the attached Information Systems Division (ISD) response to the National Automated Clearing House Association (NACHA) Draft Audit Report. We have addressed the issue listed below in our response with both a short-term and long-term solution.

- Customer Financial Information Can Be Transmitted With an Encryption Level Less Than Recommended Standard.

Please let me know if you have any questions or concerns.



STEVEN J. WESTERMAN
Deputy Director

NACHA AUDIT RESPONSE

November 17, 2008

ISSUE

DMV E-Services was contacted in early October 2008 to provide a live demonstration of the two existing internet e-commerce applications which allow DMV customers to pay for the renewal of their Vehicle Registrations and Driver License using the electronic check option (EFT). Additionally, DMV provided screen prints of the payment page(s) which reflected the current verbiage associated with an EFT transaction and also demonstrated that a customer could not proceed with the transaction until he accepted the terms and physically checked the acknowledgement 'box' to continue. See below:

By checking the box below, I hereby authorize the Department of Motor Vehicles to initiate and process a debit entry to the bank account identified above within 24 hours of this transaction. If the Department of Motor Vehicles cannot deduct the payment from my account for any reason, the Department of Motor Vehicles will charge the registered vehicle owner a service fee and any associated late payment penalties, and will attempt to collect. I will be responsible for any overdraft fees charged by my bank. Under penalty of perjury I declare that I have completed this application to the best of my knowledge and belief, it is true, correct, and complete.

☐ By checking this box I agree to the terms stated above.

To test the encryption using multiple browsers, an E-Gov developer was tasked with submitting several transactions within the different browsers/versions. Although DMV's standard is 256-AES encryption, a transaction was successfully processed in a browser which used 40-bit encryption. The NACHA minimum requirement is 128-bit encryption.

Normally, an issue such as this could be quickly addressed by the E-Gov development team. However, in addition to an E-Gov resource constraint (there is currently only one sufficiently experienced JAVA programmer and his availability is limited as a result of the XML project and WAS upgrade), DMV is in the midst of a major renovation of its web presence under the Web Site Infrastructure (WSI) project. This project is implementing a web portal presentation with an identity management component as well as restructuring the current E-Gov web applications, more specifically, the e-commerce applications are being modified to implement a 'shopping cart' functionality which will ultimately allow DMV customers to pay for multiple transactions with a single payment. When this project was begun, a 'freeze' was placed on all E-Gov web applications so that the vendor (BearingPoint) could have a baseline from which to work. Changes to these applications were to be limited to production problems, legislatively mandated items and/or business driven mandates which required immediate modifications. These changes were required to be submitted via a change control process. The vendor would evaluate the request(s) and determine if it was within the scope of approved changes during the freeze period. If any requests were deemed out-of-scope, this would allow the vendor to respond to the request with additional costs to DMV which were not covered by the existing contract.

If E-Gov were to put in server side coding to address the encryption enforcement, two applications would be involved: Driver License Internet Renewal (DLIR) and Vehicle Registration Internet Renewal (VRIR). This would affect logic within the application and would be subject to additional costs from the vendor. Below are two proposed solutions which could mitigate this issue (although a change request would still need to be submitted to the vendor).

Proposed Short-Term Solution

- DLIR/VRIR Landing Page(s) enforcing 128-bit minimum encryption level
- Verbiage within the application warning customer of security risks
- Additional verbiage within the 'TERMS' statement that customer must accept before continuing

As verbiage changes to the applications require less intervention from the WSI vendors and a JAVA resource sufficiently experienced to easily make a text change exists, a possible interim solution would be to have E-Gov developers place verbiage on the VRIR and DLIR application (appropriate) pages warning DMV online customers that to ensure the safety of their payment transaction information, browsers which support 128-bit encryption or higher are recommended. We can then provide the link to the appropriate page to download either Internet Explorer or Netscape Navigator browsers (see verbiage below currently displayed on entry pages which address browser issues with printing).

NOTE: If you are using version 4 of either Netscape Navigator or Netscape Communicator, you may not be able to print the confirmation page. We strongly suggest you upgrade from version 4 to a newer version or use a different browser to complete this transaction. You can find upgrade information [here](#).

Additionally, within the TERMS statement listed above, add verbiage stating that the customer accepts responsibility if using a browser with encryption below the 128-bit encryption level. See sample below (NOTE: This verbiage has not been approved by DMV's Legal section and/or Audit's section, it is a sample only).

By checking the box below, I hereby authorize the Department of Motor Vehicles to initiate and process a debit entry to the bank account identified above within 24 hours of this transaction. If the Department of Motor Vehicles cannot deduct the payment from my account for any reason, the Department of Motor Vehicles will charge the registered vehicle owner a service fee and any associated late payment penalties, and will attempt to collect. I will be responsible for any overdraft fees charged by my bank. Furthermore, I acknowledge that a minimum browser encryption level of 128-bit was recommended by DMV and if my browser does not meet that minimum level, DMV did provide me the opportunity, via links to supported browser levels, to upgrade my browser and process this transaction in a more secure fashion. If I chose not to upgrade my browser, I understand that the DMV cannot be held liable for any loss or damage arising from the processing of this transaction. I certify (or declare) under penalty of perjury under the laws of the State of California that the foregoing is true and correct



By checking this box I agree to the terms stated above.

DMV's Communications Program Division (CPD) is also looking into enforcing the encryption level from the landing pages of the VRIR and DLIR applications. They currently maintain the first page of the application. Their change process is much easier as they can make the changes and upload immediately into production environment. E-Gov changes require the creation of a new Java Enterprise Archive File (EAR), submission for System Testing, and coordination with Department of Technology Services (DTS) for deployment into the production environment. The manager of the team did state that although they may be able to accommodate this change, we would still need to address those customers who have bookmarked the E-Gov page as their starting point. The verbiage above is a short-term solution that can be used in conjunction with, or in place of, a CPD implemented solution.

Proposed Long Term Solution

The Web Site Infrastructure (WSI) Portal project is targeted with a tentative implementation date of December 2009. A large part of the WSI project is the security aspects which will be put in place with its deployment. Those security aspects (e.g., identity management) may address this issue with a long term solution.

In the interim, a meeting was held with DMV Java application developers on December 2, 2008. During that meeting it was determined that Java application code cannot enforce encryption levels within a customer browser. This enforcement would need to be at the application server level (currently DMV e-commerce applications reside on AIX servers at DTS). We have requested that DMV's technical liaison group (TSST) contact DTS to work on a solution whereby the application server would not allow a customer with a browser encryption level below the 128-bit minimum to continue processing an e-commerce transaction. Due to the restrictions on this type of enforcement, (e.g., There would not be a user friendly error page displayed, the customer would just receive a generic application server error), we would also have verbiage placed on several pages of the application(s) to warn customers about the minimum encryption level requirements and provide links to download the appropriate browsers. The WSI project team will be notified with the results of the TSST/DTS communication to ensure they implement a similar solution to this issue.